Jeffrey Spiegel
Scott L. Schmookler
Sara Gronkiewicz-Doran
GORDON & REES, LLP
One North Franklin
Suite 800
Chicago, Illinois 60606
(312) 565-1400
Attorneys for Federal Insurance Company

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

--X

MEDIDATA SOLUTIONS, INC.,

Plaintiff,

vs.

FEDERAL INSURANCE COMPANY,

Defendant.

--X

Civil Action No.: 1:15-cv-00907

FEDERAL INSURANCE COMPANY'S MEMORANDUM IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT (REDACTED)

TABLE OF CONTENTS

TABLE OF CONTENTS i

TABLE OF AUTHORITIES ii

INTRODUCTION 1

STATEMENT OF UNDISPUTED FACTS 3

ARGUMENT 8

I. INSURING CLAUSE 5: THE COURT OF APPEALS' BINDING PRECEDENT REQUIRES PROOF OF A HACKING– WHICH DID NOT OCCUR. 8

A. THE TRANSMISSION OF AN EMAIL IS NOT THE FRAUDULENT ENTRY OF DATA INTO A COMPUTER SYSTEM OR THE FRAUDULENT CHANGE TO DATA ELEMENTS. 9

B. THERE IS NO DIRECT NEXUS BETWEEN THE EMAILS AND THE LOSS. 13

II. INSURING CLAUSE 4: A TYPED NAME ON AN EMAIL IS NOT A FORGERY ON A FINANCIAL INSTRUMENT. 16

A. A TYPED NAMED BY AN UNIDENTIFIED SENDER IS NOT A FORGERY. 17

B. AN EMAIL DOES NOT QUALIFY AS A FINANCIAL INSTRUMENT AND THUS, CANNOT TRIGGER COVERAGE UNDER INSURING CLAUSE 4. 18

C. MEDIDATA CANNOT PROVE ITS EMPLOYEES VIEWED THE ALLEGED FORGERY. 19

III. INSURING CLAUSE 6: AN AUTHORIZED TRANSFER INITIATED AND EXECUTED BY AUTHORIZED SIGNATORIES IS NOT "FUNDS TRANSFER FRAUD." 21

A. A KNOWING TRANSFER BY AUTHORIZED SIGNATORIES IS NOT "FUNDS TRANSFER FRAUD." 21

B. INSURING CLAUSE 6 DOES NOT APPLY TO TRANSACTIONS EFFECTED BY AN EMPLOYEE. 24

CONCLUSION 25

TABLE OF AUTHORITIES

Cases

10 Ellicott Sq. Ct. Corp. v. Mountain Valley Indem. Co., 634 F.3d 112 (2d Cir. 2011) 17
Advanced Aerofoil Technologies, AG v. Todaro, 2013 WL 410873 (S.D.N.Y. Jan. 30, 2013)....24
Aetna Cas. & Sur. Co. v. Shuler, 72 A.D.2d 591 (App. Div. 1979)............23
Aetna Casualty & Surety Co. v. Kidder, Peabody & Co., 246 A.D.2d 202 (N.Y. App. Div 1998) 15
Bancinsure, Inc. v. Marshall Bank, N.A., 400 F. Supp. 2d 1140 (D. Minn. 2005) 18
Brightpoint v. Zurich Am. Ins. Co., 2006 WL 693377 (S.D. Ind. Mar. 10, 2006) 11, 15, 16
Caccioppo v. United Services Auto. Assoc., 479 N.Y.S.2d 688 (N.Y. Civ. Ct. 1984)............15
Cumberland Packing v. Chubb Ins., 958 N.Y.S.2d 306 (N.Y. Sup. Ct. 2010) 3, 22
CustomMade v. Sentinel Ins. Co., 2012 WL 4321060 (D. Mass. Sept. 17, 2012) 2, 16, 19
Elmer Fox & Co. v. Commercial Union Ins. Co., 274 F. Supp. 235(D. Colo. 1967)............17, 18
Flagstar v. Fed. Ins. Co., 2006 WL 3343765 (E.D. Mich. Nov. 17, 2006), *aff'd*, 260 Fed. Appx. 820 (6th Cir. 2008) 20
Hemi Group, LLC v. City of New York, 559 U.S. 1 (2010)............15
Hester v. Navigators Ins. Co., 917 F. Supp. 2d 290 (S.D.N.Y. 2013) 17
Intel Corp. v. Hamidi, 71 P. 3d 296 (Cal. 2003) 12
Karaduman v. Newsday, 416 N.E.2d 557 (N.Y. 1980)............23
Karakus v. Wells Fargo Bank, N.A., 941 F. Supp. 2d 318 (E.D.N.Y. 2013) 21
Metro Brokers v. Transp. Ins. Co., 2013 WL 7117840 (N.D. Ga. Nov. 21, 2013)............19
Northside Bank v. Am. Cas. Co., 60 Pa. D. & C. 4th 95 (Pa. County Ct. 2001) 22, 23
Parkans Int'l, LLC v. Zurich Ins. Co., 299 F.3d 514 (5th Cir. 2002)............19
Parma Tile v. Estate of Fred, 663 N.E.2d 633 (N.Y. 1996)............2, 16, 17, 18
Pestmaster Servs. v. Travelers Cas. & Sur. Co., 2014 WL 3844627 (C.D. Cal. July 17, 2014) .11, 22
Pinnacle Processing Group v. Hartford Cas. Ins. Co., 2011 WL 5299557 (W.D. Wash. Nov. 4, 2011)............11
Small v. Lorillard Tobacco, 252 A.D.2d 1 (N.Y. App. Div. 1998)............3, 16, 21
Spam Arrest v. Replacements, 2013 WL 4675919 (W.D. Wash. Aug. 29, 2013)............12
The Vons Co., Inc. v. Fed. Ins. Co., 57 F. Supp. 2d 933 (C.D. Cal. 1998), *aff'd*, 212 F.3d 489 (9th Cir. 2000)............19, 20
United States v. Golitschek, 808 F.2d 195 (2d Cir. 1986)............3
Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 959 N.Y.S.2d 849 (Sup. Ct. N.Y. Cty. 2013), *aff'd*, 110 A.D.3d 434 (1st Dep't 2013), *aff'd*, 2015 WL 3885816 (N.Y. June 25, 2015)............passim

INTRODUCTION

Medidata Solutions, Inc. ("Medidata") alleges that it suffered a loss after three employees allegedly misled by someone impersonating Medidata senior executive [redacted] initiated and executed an authorized wire transfer. (Dkt. 1, Complaint, ¶¶ 32-33). The impostor ***did not*** hack Medidata's computers, implant those computers with a virus, breach any firewalls or otherwise manipulate Medidata's computers. (*Id.*). Medidata seeks coverage because the thief, after verbally requesting a wire transfer, happened to confirm that request in an email. (Federal's Statement of Undisputed Material Facts ("SMF") ¶¶ 28-29, Exh. 19, 34:14-35:02, 40:09-24).[1]

Because the impostor communicated by phone and sent emails with a typed name to open unrestricted email accounts, Medidata attempts to paint the claim as computer fraud, forgery, and funds transfer fraud. It cannot, however, cite any relevant cases adopting its theories. Medidata asserts novel arguments to transform an Executive Protection Portfolio Policy (the "Policy," Exhibit 1) into all risk crime insurance that applies whenever an authorized signatory approves a wire transfer after receiving an email containing a misrepresentation.

These arguments ignore the plain terms of the Policy. The Policy provides coverage against involuntary transfers effected by hackers, forgers, and impostors; not voluntary transfers effected by authorized signatories. (SMF ¶¶ 1, 7, 10, Exh. 1). This distinction, memorialized in definitions and insuring clauses, is not novel. New York precedent existing when Medidata purchased the Policy enforces this distinction, denying the coverage Medidata demands.

First, Medidata attempts to trigger Insuring Clause 5 by characterizing the receipt of an email as "computer fraud." Insuring Clause 5, however, requires a "fraudulent entry of **Data** into … a **Computer System**" or a "fraudulent change to **Data** elements…of a **Computer**

[1] All exhibits are attached to the Parties' Joint Exhibit Stipulation.

System."[2] (SMF ¶ 9, Exh. 1, FIC001343-1344).[3] Those key phrases – fraudulent entry and fraudulent change – distinguish between an unauthorized hacking of the insured's computers and the receipt of fraudulent information. There is no debate on that issue, as the New York courts have thrice reached that conclusion. *Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.*, 959 N.Y.S.2d 849, 864 (Sup. Ct. N.Y. Cty. 2013), *aff'd*, 110 A.D.3d 434 (1st Dep't 2013), *aff'd*, 2015 WL 3885816, at *5 (N.Y. June 25, 2015). The holding in *Universal*– that the phrases "fraudulent entry" and "fraudulent change" denote a hacking – precludes coverage because Medidata never alleges a hacking; it relies entirely upon receipt of an email into an open email account. (Dkt. 1, ¶ 32-33).

Second, Medidata attempts to trigger Insuring Clause 4 by characterizing a typed name in an email as a "forgery." This theory ignores the reality that Medidata's employees do not recall seeing the name at the conclusion of the email (because the email was truncated)[4] and the typed name is not a distinctive signature. Those facts preclude coverage because (1) **Forgery** requires the imitation of a signature (not a typed name), *Parma Tile v. Estate of Fred*, 663 N.E.2d 633, 635 (N.Y. 1996); (2) the Policy only covers **Forgery** of a **Financial Instrument** (which does not include emails), *CustomMade v. Sentinel Ins. Co.*, 2012 WL 4321060, at *5 (D. Mass. Sept. 17, 2012); and (3) the truncation of the emails precludes causation, *Small v. Lorillard Tobacco*, 252

[2] Terms appearing in bold are defined terms that appear in bold in the Policy, and are bolded herein for consistency and ease of reference.

[3] Insuring Clause 5 limits coverage to "direct loss… sustained by an **Organization** resulting from **Computer Fraud** committed by a **Third Party**." (SMF ¶ 7, Exh. 1, FIC001342). The term **Computer Fraud** means the "unlawful taking or the fraudulently induced transfer of **Money**, **Securities** or **Property** resulting from a **Computer Violation**." (SMF ¶ 8, Exh. 1, FIC001343). In pertinent part, a **Computer Violation** requires "fraudulent . . . entry of **Data** into or deletion of **Data** from a **Computer System**" or "fraudulent change of **Data** elements or program logic of a **Computer System**." (SMF ¶ 9, Exh. 1, FIC001343-FIC001344)

[4] (SMF ¶ 26, Exh. 20, 27:03-10, 28:06-09; SMF ¶ 39, Exh. 21, 38:04-16; SMF ¶ 40, Exh. 19, 42:16-22).

A.D.2d 1, 10 (N.Y. App. Div. 1998).

Third, Medidata attempts to trigger Insuring Clause 6 on the theory that a wire transfer effected by its authorized signatories is **Funds Transfer Fraud**. That defined term, however, requires proof that someone impersonating the insured instructed the bank to transfer funds, and does not apply to transfers voluntarily effected by Medidata. *Cumberland Packing v. Chubb Ins.*, 958 N.Y.S.2d 306 (N.Y. Sup. Ct. 2010). As in *Cumberland*, Medidata's employees manually entered and approved the claimed wire transfer (Dkt. 1, ¶ 32-33) and thus, it cannot trigger coverage. *Id.*

Medidata purchased the Policy after New York courts held that similar insuring agreements do not cover transfers caused by misrepresentations. *United States v. Golitschek*, 808 F.2d 195, 202-03 (2d Cir. 1986) (a party is deemed to know existing law). Having elected this coverage, Medidata cannot now attempt to circumvent the policy it purchased. Applying the plain terms of the Policy as interpreted by New York courts, Federal Insurance Company asks that this Court enter summary judgment in its favor and against Medidata.

STATEMENT OF UNDISPUTED FACTS

Medidata alleges that its employees were (on September 16, 2014) tricked into wire transferring $4,770,226.00 to a bank account in China. (Dkt. 1, ¶ 32-33). Medidata's complaint emphasizes the receipt of emails, but discovery proved that the receipt of emails was not the operative event resulting in the transfer of funds. Medidata's employees, acting within their authority, voluntarily executed the wire transfer (SMF ¶ 32, Exh. 20, 13:20-14:16, 50:17-51:14, 53:06-54:20; SMF ¶ 48, Exh. 21, 32:10-25, 48:24-49:21; SMF ¶ 49, Exh. 19, 57:13-58:16) based upon verbal discussions and independent knowledge of a legitimate acquisition. (SMF ¶ 31, Exh. 20, 25:20-26:06; SMF ¶ 45, Exh. 21, 30:07-16; SMF ¶ 51, Exh. 19, 51:05-21).

A. INITIATION OF THE CLAIMED TRANSFER

Medidata employed [redacted] [redacted] ("[redacted]") as an [redacted]. (SMF ¶ 13, Exh. 20, 10:12-13). In this capacity, [redacted] was authorized to process invoices for payment and prepare wire transfers for approval. (SMF ¶¶ 14-15, Exh. 20, 10:14-18, 11:18-22). She was not, however, authorized to approve wire transfers. (SMF ¶ 17, Exh. 20, 11:15-18). Wire transfers had to be approved by at least one authorized signatory. (SMF ¶ 18, Exh. 20, 12:06-12:10).

On September 16, 2014, [redacted] received an email purportedly sent by a Medidata executive, [redacted] ("[redacted]"). (SMF ¶ 24, Exh. 20, 26:07-21). This email did not request or authorize the transfer of money; it made no reference to the transfer of money. It simply stated that "[i]n regards to an Acquisition that we are currently undergoing, Attorney Michael Meyer (mmeyer@consultant.com) is going to be contacting you. If you can please devote your full attention to his demand to acquire some accounting information so that we can finalize this deal." (SMF ¶ 25, Exh. 2).

After receiving the initial email, someone claiming to be Michael Meyer ("Meyer") contacted [redacted] via telephone . (SMF ¶ 27, Exh. 20, 30:23-31:13). During their telephone discussion, Meyer asked [redacted] to process a wire transfer. (SMF ¶ 28, Exh. 20, 34:14-35:02). Prior to that verbal request, [redacted] had not received an email directing her to transfer any money:

> Q. Do you recall if the first mention of transferring money was over the phone during one of these phone conversations?
> A. Yes, I think it was. . . .
> Q. So, from a chronology perspective, the first mention of wire transferring money was in a phone call which was then followed up with an e-mail?
> A. Yeah, I believe so.

(*Id.*). [redacted] asked Meyer to arrange for a written confirmation of the transfer, and suggested that [redacted] send an email confirming the requested transfer to her and two authorized signatories (the names of whom she provided). (SMF ¶ 28, Exh. 20, 34:14-35:02; SMF ¶ 30, Exh. 5).[5]

Thereafter, [redacted] logged into Chase's on-line banking system to initiate the transfer. (SMF ¶ 32, Exh. 20, 13:20-14:16). This process was manual. [redacted] input her assigned login and password, and a random code assigned by a fob (a small token that assigns a code every few seconds) Chase assigned to her. (SMF ¶ 32, Exh. 20, 50:17-51:14, 53:06-54:20). Relying upon knowledge of internal discussions,[6] [redacted] entered the wire transfer into the Chase banking system (*Id.*), and submitted it for approval by two other Medidata employees, [redacted] ("[redacted]") and [redacted] ("[redacted]"). (SMF ¶ 23, Exh. 20, 15:11-23, 16:17-17:05).

B. Approval of the Claimed Transfer

[redacted], the [redacted] (SMF ¶ 33, Exh. 21, 9:02-10:02), was an authorized signatory on Medidata's bank account at Chase. (SMF ¶ 34, Exh. 21, 10:19-25). As an authorized signatory, [redacted] had access to Chase's on-line banking system. (SMF ¶ 41, Exh. 21, 11:21-25, 12:05-17). Like [redacted], [redacted] could only access the system by using his unique login and password, and a random code assigned by a fob (which [redacted] kept in his office). (SMF ¶ 42, Exh. 21, 12:18-13:19, 14:09-20). Once he logged in, [redacted] could review and approve pending wire transfers. (SMF ¶ 42, Exh. 21, 13:20-14:08).

On September 16, [redacted] notified [redacted] that she needed him to approve a wire transfer. (SMF ¶ 44, Exh. 20, 23:15-18). [redacted] then logged into Chase's system and approved the wire transfer. (SMF ¶ 47, Exh. 21, 32:10-25, 48:24-49:21). That approval was not, however, sufficient to complete the transaction because the transfer required two approvals. (SMF ¶ 48,

[5] The impostor subsequently sent another email to [redacted] providing the beneficiary details for the transaction they discussed on the telephone. (SMF ¶ 29, Exh. 20, 40:09-24; Exh. 8).

[6] [redacted] did not verify the legitimacy of the transfer because Medidata's senior management mentioned the possibility of acquiring a company and told the accounting department to be ready to process the acquisition on an expedited basis. (SMF ¶ 31, Exh. 20, 25:20-26:06). [redacted] assumed that the requested transfer related to a legitimate acquisition and therefore, initiated it without requesting or reviewing any source documentation. (*Id.*)

Exh. 21, 51:10-51:15). The wire transfer had to be released by a second signatory. (*Id.*)

[redacted], Medidata's former [redacted], was also an authorized signatory on Medidata's account with Chase. (SMF ¶¶ 35-36, Exh. 19, 10:25-11:05, 11:23-12:02). As an authorized signatory, [redacted] had access to Chase's on-line banking system. (SMF ¶ 49, Exh. 19, 57:13-58:16). Like [redacted], [redacted] could only access the system by logging in with a unique login and password and a random code assigned by a fob. (*Id.*). Once he logged in, he could review and release pending wire transfers. (*Id.*).

After [redacted] approved the wire transfer (SMF ¶ 47, Exh. 21, 32:10-25, 48:24-49:21), [redacted] released the wire transfer. (SMF ¶ 52, Exh. 19, 59:16-18, 60:02-04). Like [redacted], [redacted] did not independently verify the transaction[7] because he knew that Medidata was conducting a legitimate acquisition of a company and the size of the wire was consistent with that transaction:

> Q. Did you at the time of the wire have any idea why 4 plus million dollars was being wire transferred?
> A. I assumed something.
> Q. What did you assume?
> A. That it was for an acquisition that was in play.
> Q. When you say acquisition, what are you talking about?
> A. We were going through an M and A transaction at the time about the same size.
> Q. When you say M and A transaction what are you referring to?
> A. Meaning we were in a process of acquiring an organization.
> Q. So Medidata was purchasing a company?
> A. Yes.

(SMF ¶ 53, Exh. 19, 36:25-37:17). Knowledge of Medidata's purchase of a company was the only reason he approved the transfer:

[7] [redacted] and [redacted] verbally discussed the requested transfer. [redacted] asked whether [redacted] had actually spoken with "him," meaning [redacted]. (SMF ¶ 51; Exh. 19, 51:05-21). [redacted] thought that "him" referred to Meyer, and confirmed that she had spoken to "him." SMF ¶ 50, Exh. 19, 57:13-58:16). Based upon [redacted]' verbal representation, [redacted] logged into the Chase banking system, and approved the transfer. (*Id.*).

Q. But the only reason you approved this wire is because it was your impression that this was funding an existing purchase Medidata was actually going through?
MR. ZIFFER: Objection.
A. Yes.

(SMF ¶ 54, Exh. 19, 56:04-09).

C. Discovery of the Claimed Fraud

Medidata suggests that its employees were not aware of the fraud because the emails appeared to be sent from [redacted] legitimate email account. (Dkt. 1, ¶ 3). However, the emails identified the "reply to" address and [redacted] legitimate email address was not identified in the "reply to" field. (SMF ¶ 60, Exh. 19, 46:08-24). The "reply to" field contained a foreign email address (secureop@dr.com). (*Id.*).

This is the fact that led Medidata to terminate a second transfer. On September 18, 2014, the person claiming to be Meyer contacted [redacted] again about a second wire transfer. (SMF ¶ 58, Exh. 20, 42:02-10). [redacted] initiated the wire transfer and [redacted] approved it (SMF ¶ 59; Exh. 21, 40:24-41:20), but [redacted] rejected the transaction because the email address in the "reply to" field was not a Medidata address, which suggested an illegitimate transaction:

Q. So back to my question. The e-mail at 3:34, the to address, meaning secureop@dr.com, it's that address that led you to conclude that the subsequent attempt later in September was illegitimate?
A. Yes.
Q. And as I understand it, what made you reach that conclusion is secureop@dr.com is nothing related to Medidata?
A. Correct.
Q. And so just by looking at that address you could tell immediately this is not something legitimate?
A. I couldn't tell if it was something that was illegitimate. There was something that was definitely not correct about the e-mail. So I wanted to make sure that it was okay.

(SMF ¶ 60, Exh. 19, 46:08-24).

[redacted] contacted [redacted] to confirm that he intended to initiate the September 18, 2014 transaction. (SMF ¶ 61, Exh. 19, 64:11-65:07). When he denied knowledge of the transaction, Medidata terminated the second wire transfer. (*Id.*). The same secureop@dr.com email address in the "reply to" field also appeared on the September 16 emails. (SMF ¶ 60, Exh. 19, 46:08-24).

ARGUMENT

Although Medidata's authorized signatories voluntarily processed and approved the wire transfer (SMF ¶ 32, Exh. 20, 13:20-14:16, 50:17-51:14, 53:06-54:20; SMF ¶ 48, Exh. 21, 32:10-25, 48:24-49:21; SMF ¶ 49, Exh. 19, 57:13-58:16), Medidata seeks coverage on the theory that its employees received a truncated email relating to a wire transfer originally requested over the phone and because (theoretically) the expansion of the email would reveal a typed name.

Medidata cannot meet its burden[8] of proving, through admissible evidence, each element of coverage under the Policy because: (1) a voluntary and authorized transfer is not **Computer Fraud** under Insuring Clause 5; (2) a typed name in a truncated email is not a **Forgery** on a **Financial Instrument** under Insuring Clause 4; and (3) an authorized transfer executed by authorized signatories is not **Funds Transfer Fraud** under Insuring Clause 6.

I. <u>INSURING CLAUSE 5</u>: THE COURT OF APPEALS' BINDING PRECEDENT REQUIRES PROOF OF A HACKING– WHICH DID NOT OCCUR.

Medidata's claim under Insuring Clause 5 rests on the notion that the Policy covers any transfer tangentially related to an email containing false information. This theory ignores the plain language of the insuring clause and the incorporated definitions. That is why *Universal* rejected an analogous argument and conclusively held that computer fraud coverage does not apply absent a hacking incident – which did not occur. 2015 WL 3885816 at *4-5.

As in *Universal*, Insuring Clause 5 differentiates between voluntary transfers effected by

[8] *Morgan Stanley v. New England Ins. Co.*, 225 F.3d 270, 276 (2d Cir. 2000) ("a policyholder bears the burden of showing that the insurance contract covers his loss").

the insured and involuntary transfers effected by a hacker. It does so by limiting coverage to "direct loss… sustained by an **Organization** resulting from **Computer Fraud** committed by a **Third Party**." (SMF ¶ 7, Exh. 1, FIC001342). **Computer Fraud** means the "unlawful taking or the fraudulently induced transfer of **Money**, **Securities** or **Property** resulting from a **Computer Violation**." (SMF ¶ 8, Exh. 1, FIC001343). It is not, therefore, enough for Medidata to allege a fraud involving a computer. It must prove a **Computer Violation**, defined as the "fraudulent:

> (1) entry of **Data** into or deletion of **Data** from a **Computer System**;
>
> (2) change to **Data** elements or program logic of a **Computer System**, which is kept in machine readable format; or
>
> (3) introduction of instructions, programmatic or otherwise, which propagate themselves through a **Computer System**;
>
> directed against an **Organization**."

(SMF ¶ 9, Exh. 1, FIC001343-1344).

Medidata cannot meet its burden because (1) the transmission of an email into an open inbox is not a **Computer Violation**, and (2) the loss did not result from the receipt of the email.

A. The Transmission of an Email Is Not the Fraudulent Entry of Data Into a Computer System or The Fraudulent Change to Data Elements.

Medidata alleges that the subject emails are either the "fraudulent entry of **Data**" or "fraudulent change to **Data** elements." (Dkt. 1, ¶ 38).[9] The Court of Appeals resolved any questions about the meaning of these phrases in *Universal* – unconditionally holding that the phrases "fraudulent entry" or "fraudulent change" denote a hacking and require proof of an unauthorized entry into the insured's computer system. 2015 WL 3885816 at *4-5. No such

[9] Medidata's complaint only alleges coverage under subsections (1) and (2) of the definition of **Computer Violation** and thus, Federal will only address those subsections.

unauthorized entry occurred in this case. Medidata's claim rests on the sending of an email to an open email inbox. (Dkt. 1, ¶ 32-33). This theory fails because the Court of Appeals rejected the notion that receipt of false information constitutes a "fraudulent entry" or a "fraudulent change."

Universal, which has been consistent across three layers of judicial scrutiny, demonstrates why Medidata's claim is not covered. In that case, the thief entered fraudulent information into the insured's computer system, prompting the computer to automatically issue a series of payments. Despite these facts, the court denied coverage because the insuring agreement only provided coverage for a "fraudulent entry of Electronic Data…or change of Electronic Data" (959 N.Y.S.2d at 861):

> [T]he Rider states that it covers "fraudulent entry" of data or computer programs into Universal's computer system which resulted in a loss. This indicates that coverage is for an unauthorized entry into the system, i.e. by an unauthorized user, such as a hacker, or for unauthorized data, e.g. a computer virus.

Universal, 959 N.Y.S.2d at 864.

The Appellate Division affirmed that analysis. Rejecting the notion that the policy covers any loss that arises from the electronic receipt of fraudulent information, the Appellate Division agreed that "fraudulent entry" or "fraudulent change" references a hacking: "[t]he court correctly found that the unambiguous plain meaning of defendant's computer systems fraud rider, covering loss from a fraudulent 'entry of electronic data' or 'change of electronic data' within the insured's proprietary computer system, was intended to apply to wrongful acts in manipulation of the computer system, i.e., by hackers. . . ." *Id.*, 110 A.D.3d at 434.

The Court of Appeals affirmed the lower courts' holdings. Focusing on the fact that the term "fraudulent" modified the words "entry" and "change," the court held that the insured could not pursue coverage simply because a thief entered fraudulent information into the insured's computer. The phrases "fraudulent entry" or "fraudulent change," the court concluded, denoted a hacking of the insured's computer:

> In the Rider, "fraudulent" modifies "entry" or "change" of electronic data or computer program, meaning it qualifies the act of entering or changing data or a computer program. Thus, the Rider covers losses resulting from a dishonest entry or change of electronic data or computer program, constituting what the parties agree would be "hacking" of the computer system. The Rider's reference to "fraudulent" does not also qualify what is actually acted upon, namely the "electronic data" or "computer program" itself. The intentional word placement of "fraudulent" before "entry" and "change" manifests the parties' intent to provide coverage for a violation of the integrity of the computer system through deceitful and dishonest access.

Universal, 2015 WL 3885816 at *5.

While the common law term "fraud" may be broad, the Policy does not apply to all common law frauds. It requires more. The phrases "fraudulent entry" or "fraudulent change" impose a stringent condition on coverage that is not satisfied by receipt of fraudulent information through an electronic source (which is the extent of the link between the emails and Medidata's transfer of funds). *See, e.g. Pestmaster Servs. v. Travelers Cas. & Sur. Co.*, 2014 WL 3844627, at *6-7 (C.D. Cal. July 17, 2014); *Pinnacle Processing Group v. Hartford Cas. Ins. Co.*, 2011 WL 5299557, at *6 (W.D. Wash. Nov. 4, 2011); *Brightpoint v. Zurich Am. Ins. Co.*, 2006 WL 693377, at *7 (S.D. Ind. Mar. 10, 2006).

Pestmaster explained why the receipt of fraudulent information (even if it persuades an employee to approve a transfer) does not trigger coverage. In that case, the court held that there was no coverage under a computer fraud insuring clause where an insured paid funds based on falsified invoices submitted electronically. Relying in part on *Universal*, the court held that the insuring agreement applied "when someone 'hacks' or obtains unauthorized access or entry to a computer in order to make an unauthorized transfer or otherwise uses a computer to fraudulently cause a transfer of funds." *Id.*, 2014 WL 3844627 at *6. The court drew a distinction between an involuntary transfer and a voluntary transfer brought about through fraud:

> However, there is an important distinction between "fraudulently causing a transfer," as "Computer Fraud" is described in the Policy, and Pestmaster's interpretation of "Computer Fraud" as "causing a fraudulent transfer." . . . In this case, it is undisputed that Pestmaster authorized Priority 1 to initiate ACH transfers from its account to Priority 1's account so that Priority 1 could pay Pestmaster's payroll and payroll taxes. In its Opposition, Pestmaster does not argue—nor could it—that Priority 1 was an unauthorized user or hacker or that Priority 1 somehow subverted Pestmaster's computer in the actual transfer of funds into Priority 1's account. . . . Therefore, Priority 1's conduct does not constitute "Computer Fraud" as defined by the Policy because the transfer of funds was at all times authorized and did not involve hacking or any unauthorized entry into a computer system.

Id. at *6.

Universal refutes Medidata's claim because it provides a definitive interpretation of the phrases "fraudulent entry" and "fraudulent change" and conclusively establishes that these phrases require proof of a hacking – which Medidata does not allege. (Dkt. 1, ¶ 32-33). The receipt of an email cannot constitute a "fraudulent entry" and a "fraudulent change" because email accounts are open repositories, over which Medidata chose to place no restrictions.[10] Anyone was free to transmit emails to Medidata, and their doing so is not an accessing of Medidata's system or the fraudulent entry therein. *See, e.g. Intel Corp. v. Hamidi*, 71 P. 3d 296, 304 (Cal. 2003) ("sending of electronic communications that assertedly cause injury only because of their contents" is not "an actionable trespass to a computer system through which messages are transmitted"); *Spam Arrest v. Replacements*, 2013 WL 4675919, *68 (W.D. Wash. Aug. 29, 2013) ("no Ninth Circuit court has ever held that the mere act of sending an email constitutes access to a computer through which the email passes on the way to its recipient.").

This is the foundation for *Universal*. *Universal* held that an automated transfer resulting

[10] Prior to the loss, Medidata had the opportunity to implement an electronic control which would have inhibited the spoofing of emails and blocked unwanted emails, but it did not implement this control prior to the loss (SMF ¶ 65, Exh. 16; SMF ¶ 66, Exh. 17) and chose not to train its employees on avoiding this type of fraud. (SMF ¶ 62, Exh. 20, 8:24-0:02; SMF ¶ 63, Exh. 21, 52:21-23; SMF ¶ 64, Exh. 19, 10:04-08).

from the direct entry of fraudulent information into the insured's computer system did not trigger coverage because the receipt of fraudulent information did not constitute a "fraudulent entry" of data or "fraudulent change" to data. *Id.*, 2015 WL 3885816 at *1-2. Medidata's claimed loss, unlike the loss in *Universal*, did not involve an automated transfer unknowingly resulting from fraudulent information. *Id.* at *3 ("claims submitted are processed, approved, and paid automatically, without manual review"). It involved a voluntary transfer input and approved by authorized users. (SMF ¶ 32, Exh. 20, 13:20-14:16, 50:17-51:14, 53:06-54:20; SMF ¶ 48, Exh. 21, 32:10-25, 48:24-49:21; SMF ¶ 49, Exh. 19, 57:13-58:16). Thus, Medidata cannot establish a threshold for coverage (a **Computer Violation)** and its claim under Insuring Clause 5 fails.

B. THERE IS NO DIRECT NEXUS BETWEEN THE EMAILS AND THE LOSS.

Medidata's inability to prove a **Computer Violation** is only one reason its claim fails under Insuring Clause 5. Medidata's claim also fails because Medidata cannot prove a causal nexus between the emails and the wire transfer. Emails cannot initiate a wire transfer by themselves. (SMF ¶¶ 55-56, Exh. 19, 32:12-24, 47:15-22). On the contrary, a wire transfer requires three employees (using three different logins, three different passwords and three different encryption codes) to manually access an online banking program. (SMF ¶¶ 15-20, Exh. 20, 11:18-22, 11:12-14, 11:15-18, 12:06-10, 13:07-19, 13:20-14:16; SMF ¶¶ 41-42, Exh. 21, 11:21-25, 12:05-17, 12:18-13:19, 14:09-20; SMF ¶ 49, Exh. 19, 57:13-58:16). Given that the direct accessing of the insured's system resulting in an automatic transfer of funds to the fraudsters in *Universal* was insufficient to trigger coverage (2015 WL 3885816 at *1), the receipt of an email – which could not itself result in a transfer of funds – does not do so.

Medidata emphasizes the receipt of fraudulent emails, but its employees testified that the email alone was not enough to persuade them to initiate the wire transfer. [redacted], the person who released the wire and whose approval was necessary to complete the transaction, proceeded with the transaction because [redacted] told him that she verbally confirmed the transaction and he was aware of a legitimate transaction. (SMF ¶¶ 51, 53, Exh. 19, 51:05-21, 36:25-37:17). The latter, according to [redacted], was the "only" reason he approved the transfer:

> Q. But the only reason you approved this wire is because it was your impression that this was funding an existing purchase Medidata was actually going through?
> MR. ZIFFER: Objection.
> A. Yes.

(SMF ¶ 54, Exh. 19, 56:04-09).

This testimony demonstrates the remoteness between the email and the transfer. The email – received after a telephone conversation – was followed by the following steps:

Step 1: [redacted] logs into Chase's system using login, password, and encryption key (SMF ¶ 32, Exh. 20, 13:20-14:16, 50:17-51:14, 53:06-54:20);

Step 2: [redacted] sets up wire transfer and transmits to [redacted] (SMF ¶ 22, Exh. 20, 15:11-23, 16:17-17:05);

Step 3: [redacted] discusses wire transfer with [redacted] (SMF ¶ 46, Exh. 20, 43:04-08);

Step 4: [redacted] logs into Chase's system using login, password, and encryption key (SMF ¶ 42, Exh. 21, 12:18-13:19, 14:09-20);

Step 5: [redacted] reviews and approves wire transfer (SMF ¶ 43, Exh. 21, 13:20-14:08);

Step 6: [redacted] discusses wire transfer with [redacted] and [redacted] (SMF ¶ 44, Exh. 21, 30:07-16;

Step 7: [redacted] relates wire to pending transaction (SMF ¶ 53, Exh. 19, 36:25-37:17);

Step 8: [redacted] logs into Chase's system using login, password, and encryption key (SMF ¶ 49, Exh. 19, 57:13-58:16); and

Step 9: [redacted] reviews and releases wire transfer (SMF ¶ 54, Exh. 19, 56:04-09).

These steps are fatal to Medidata's claim because Insuring Clause 5 requires a causal nexus between the alleged fraudulent entry or fraudulent change and the loss: "direct loss…

sustained by an **Organization** resulting from **Computer Fraud** committed by a **Third Party**." (SMF ¶ 7, Exh. 1, FIC001342). No such nexus exists because [redacted] approval was based upon his knowledge of a legitimate corporate transaction and a verbal conversation with [redacted]. (SMF ¶¶ 51, 53-54, Exh. 19, 51:05-21, 36:25-37:17, 59:56:04-09). Those events – neither of which were electronic – were the seminal events which resulted in the approval of the transfer of funds.

Under New York law, the attenuated connection between the initial receipt of emails confirming a verbal request and the ultimate transfer of funds is insufficient to establish the causal relationship necessary for coverage under the Policy. *Aetna Casualty & Surety Co. v. Kidder, Peabody & Co.*, 246 A.D.2d 202, 209 (N.Y. App. Div 1998). Even in tort, "proximate cause . . . requires 'some direct relation between the injury asserted and the injurious conduct alleged.'" *Hemi Group, LLC v. City of New York*, 559 U.S. 1, 9 (2010). A link that is "'too remote,' 'purely contingent,' or 'indirec[t]' is insufficient." *Id.* In light of the facts disclosed during the depositions of the involved Medidata employees, Medidata cannot show that the transfer resulted from the receipt of the emails because at each step, Medidata's employees considered the request to transfer funds. *See Caccioppo v. United Services Auto. Assoc.*, 479 N.Y.S.2d 688, 689-690 (N.Y. Civ. Ct. 1984).

The decision in *Brightpoint* illustrates the flaw in Medidata's claim. 2006 WL 693377 at *7. In that case, the insured's subsidiary was a wholesale distributor of prepaid mobile telephone cards. The subsidiary received, by facsimile, purchase orders, post-dated checks, and guaranties thought to be from a dealer. After receiving the faxed orders, the insured purchased phone cards, which it then sent to the thief. When the dealer denied authorizing the transaction, the insured sought coverage under its crime policy. The insurer denied coverage because the insured could not establish a sufficient nexus between the facsimile and the loss. The court agreed, denying coverage because the insured's loss did not flow immediately from the use of the facsimile machine. The court noted that the facsimile "simply alerted the company" that someone wished to place an order, but that under the insured's procedure "the cards would not have been turned over simply on the basis of the facsimile." *Id.* The court thus held that intervening events were the direct, proximate, predominate, and immediate cause of the insured's loss.

Just as in *Brightpoint*, the subject emails did not create, authorize, or release a wire transfer. [redacted] testified that he would not have proceeded based upon the email. (SMF ¶ 54, Exh. 19, 68:10-14). The subject wire transfer required intervening steps (in which each of the three employees manually logged into Chase's banking system to create, approve, and release a wire transfer)[11] and was approved "only" because of a verbal discussion and [redacted] knowledge of Medidata's on-going business transactions. (SMF ¶¶ 51, 53-54, Exh. 19, 51:05-21, 36:25-37:17, 59:56:04-09). Because these determinative events did not involve the email, Medidata cannot establish that the claimed loss resulted from a **Computer Violation**.

II. INSURING CLAUSE 4: A TYPED NAME ON AN EMAIL IS NOT A FORGERY ON A FINANCIAL INSTRUMENT.

Medidata seeks coverage under Insuring Clause 4 on the theory that the subject emails bear a forgery. (Dkt. 1, ¶ 40). This theory ignores the terms of Insuring Clause 4, which conditions coverage upon proof of a "direct loss . . . resulting from **Forgery** or alteration of a **Financial Instrument** committed by a **Third Party**. . . ." (SMF ¶ 2, Exh. 1, FIC001342). Medidata cannot establish these elements because: (1) the emails do not contain a signature and thus, do not bear a **Forgery**, *Parma Tile*, 663 N.E.2d at 635; (2) the emails do not contain a promise to pay money and thus, do not qualify as a **Financial Instrument**, *CustomMade*, 2012 WL 4321060 at *5; and (3) Medidata cannot prove that its employees saw the alleged forgery

[11] (SMF ¶ 32, Exh. 20, 13:20-14:16, 50:17-51:14, 53:06-54:20; SMF ¶ 48, Exh. 21, 32:10-25, 48:24-49:21; SMF ¶ 49, Exh. 19, 57:13-58:16)

and thus, cannot prove a loss resulting from a **Forgery**, *Small*, 252 A.D.2d at 10.

A. A TYPED NAMED BY AN UNIDENTIFIED SENDER IS NOT A FORGERY.

Medidata's Insuring Clause 4 claim depends upon the notion that typing a name at the conclusion of an email constitutes a **Forgery**, as defined by the Policy. That suggestion, however, is an improper attempt to rewrite the clear terms of the Policy, in violation of settled rules of contract interpretation. *Hester v. Navigators Ins. Co.*, 917 F. Supp. 2d 290, 296-298 (S.D.N.Y. 2013) ("the unambiguous provisions of the policy must be given their plain and ordinary meaning"; a court "cannot rewrite the plain terms of the Policy"). The Policy does not define **Forgery** to mean merely the typing of another person's name. **Forgery** means the

> [S]igning of the name of another natural person or organization, with the intent to deceive, but does not mean a signature that includes, in whole or in part, one's own name, with or without authority, in any capacity for any purpose. Mechanically or electronically produced or reproduced signatures shall be treated the same as hand-written signatures.

(SMF ¶ 3, Exh. 1, FIC001345).

Medidata's theory ignores the definition's reference to "signature." The use of that term differentiates between typing of a name and the distinctive signing of a name. "Signature" means "a person's name written in that person's handwriting" (www.merriam-webster.com) or "a person's name written in a distinctive way as a form of identification in authorizing a check or document or concluding a letter." (www.oxforddictionaries.com; *see also* http://en.wikipedia.orn/wiki/Signature).[12] A typed name is not a distinctive or stylized presentation of the person's name. *See, e.g., Parma Tile*, 663 N.E.2d at 635; *Elmer Fox & Co. v. Commercial Union Ins. Co.*, 274 F. Supp. 235, 239-240 (D. Colo. 1967).

Parma Tile refutes the notion that the electronic addition of a name constitutes a

[12] *10 Ellicott Sq. Ct. Corp. v. Mountain Valley Indem. Co.*, 634 F.3d 112, 120 (2d Cir. 2011) ("it is common practice for the courts of [New York] State to refer to the dictionary to determine the plain and ordinary meaning of words to a contract").

signature. In that case, the plaintiff argued that a document sent via facsimile bore a "signature" because the defendant programmed a fax machine to imprint its name on every page. Nonetheless, the Court of Appeals rejected the notion that the typed name constituted a "signature." *Id.*, 663 N.E.2d at 634-35.

Elmer Fox reached the same conclusion while interpreting forgery coverage. The bank argued that a check was forged because it was endorsed with a stamp containing the payee's name. The court disagreed, holding that a stamped name was not a signature: "[The] rubber stamp endorsement consists of the words "For deposit only" with the name and address of the company. This is not a signature." 274 F. Supp. at 240.[13]

Consistent with *Parma*, the typewritten word "[redacted]" at the conclusion of an email is not a replication of "[redacted]" handwritten signature and does not have any of the attributes of a signature by "[redacted]." It does not, therefore, qualify as a signature and cannot qualify as a **Forgery** under the Policy. Thus, Medidata's Insuring Clause 4 claim fails as a matter of law.

B. An Email Does Not Qualify as a Financial Instrument and thus, Cannot Trigger Coverage Under Insuring Clause 4.

Proof of a **Forgery** is only one required element of coverage under Insuring Clause 4. Limiting coverage to a **Forgery** on a specific type of document, Insuring Clause 4 requires "**Forgery** . . . of a **Financial Instrument** committed by a **Third Party**." (SMF ¶ 2, Exh. 1, FIC001342). **Financial Instrument** does not encompass an email. It is defined to mean a "check, draft or similar written promise, order or direction to pay a sum certain in **Money** that is

[13] While the Policy's definition of **Forgery** references "mechanically" reproduced signatures, this phrase does not encompass the typing of a name in an email. This phrase encompasses "'a signature that has been prepared and reproduced by mechanical or photographic means,' in other words, a signature that was generated by some mechanical process, rather than by a handwriting." *Bancinsure, Inc. v. Marshall Bank, N.A.*, 400 F. Supp. 2d 1140, 1143-1144 (D. Minn. 2005). The Policy contains examples of mechanically or electronically produced or reproduced signatures of Federal's representatives. (SMF ¶ 12, Exh. 1, FIC001328).

made, drawn by or drawn upon an **Organization** or made or drawn by anyone acting as an **Organization's** agent, or that is purported to have been so made or drawn." (SMF ¶ 4, Exh. 1, FIC001345).

This definition encompasses documents that "have traditionally been those with legal effect, documents that can be 'deposited.'" *The Vons Co., Inc. v. Fed. Ins. Co.*, 57 F. Supp. 2d 933 (C.D. Cal. 1998), *aff'd*, 212 F.3d 489 (9th Cir. 2000). An email does not satisfy this test because unlike a check it: (1) lacks a drawer, drawee, and payee; (2) is not depositable into a bank account by the recipient; and (3) does not contain a promise to pay money. *Parkans Int'l, LLC v. Zurich Ins. Co.*, 299 F.3d 514 (5th Cir. 2002); *CustomMade*, 2012 WL 4321060 at *5; *Metro Brokers v. Transp. Ins. Co.*, 2013 WL 7117840, at *5 (N.D. Ga. Nov. 21, 2013).

CustomMade rejected an analogous attempt to trigger forgery coverage. In that case, the court held that an altered email did not trigger coverage because an email is not a qualifying document. *Id.* at *5. The court explained that "Engelman could not take the e-mail to a bank and demand payment, just as he could not use an IOU from CustomMade written on a scrap of paper to pay his credit card bill. Thus, it is not of the same kind or class as a 'check, draft, or promissory note.'" *Id.* at *5; *Metro Brokers*, 2013 WL 7117840 at *5 (electronic transfers did not trigger coverage because they were not checks, drafts, promissory notes, bills of exchange, or similar written promises, orders, or directions to pay a sum certain).

Medidata cannot trigger coverage by volleying allegations of **Forgery** based on the alleged typing of a name into an email. Because an email is not a **Financial Instrument**, an alleged forgery thereon does not trigger coverage and Medidata's claim fails as a matter of law.

C. Medidata Cannot Prove Its Employees Viewed the Alleged Forgery.

While Medidata's inability to prove a **Forgery** on a qualifying document precludes coverage, Medidata's claim would fail (even if the Court accepted this thesis) because Medidata cannot even prove that [redacted], [redacted], or [redacted] saw the alleged forgery. The typed name Medidata characterizes as forged was truncated in the subject emails (SMF ¶ 24, Exh. 2; SMF ¶ 29, Exh. 8) and could only be viewed by expanding the emails.[14] [redacted], [redacted], and [redacted], however, could not recall expanding the email to see the typed name. (SMF ¶ 26, Exh. 20, 27:03-10, 28:06-09; SMF ¶ 39, Exh. 21, 38:04-16; SMF ¶ 40, Exh. 19, 42:16-22).

This admission is fatal to Medidata's claim because Insuring Clause 4 requires proof of "direct loss sustained by an **Organization** resulting from **Forgery** or alteration of a **Financial Instrument** committed by a **Third Party**." (SMF ¶ 2, Exh. 1, FIC001342). Medidata cannot prove causation (*i.e.*, a direct loss resulting from a **Forgery**) because it cannot even prove that its employees saw the alleged forgery, let alone that the alleged forgery caused the wire transfer. *Flagstar v. Fed. Ins. Co.*, 2006 WL 3343765, at *8 (E.D. Mich. Nov. 17, 2006), *aff'd*, 260 Fed. Appx. 820, 824 (6th Cir. 2008); *Vons*, 57 F. Supp. 2d at 946; *Simon Marketing v. Gulf Ins. Co.*, 149 Cal. App. 4th 616, 623 (Cal. Ct. App. 2007).

Flagstar rejected the notion that the mere existence of a forgery, without proof of causation, triggers coverage. In that case, the insured proved that it received forged notes, but the court nonetheless held that there was no coverage because the insured could not prove that it would not have sustained the same loss absent the forgeries (because the notes were not enforceable for lack of consideration, even if legitimately signed). *Flagstar*, 2006 WL 3343765 at *8 (that the insured would not have parted with the funds absent the forgery "at most proves that [the insured] considered the notes to be important," but not causation).

Medidata's inability to prove that its employees even saw the typed name in the emails

[14] The truncation is identified with an ellipsis. Medidata's employees testified that they could only see that portion of the email if they clicked on the ellipsis. (SMF ¶ 26, Exh. 21, 27:03-10; SMF ¶ 40, Exh. 19, 40:23-41:08).

precludes a showing of causation, as New York courts routinely reject the notion that an unseen statement can cause a loss. *See, e.g. Small,* 252 A.D.2d at 10 (without proof that plaintiffs actually viewed fraudulent statements, they could not establish causation); *Karakus v. Wells Fargo Bank, N.A.*, 941 F. Supp. 2d 318, 341 (E.D.N.Y. 2013) (causation was "lacking" because plaintiff affirmed that she "did not even read the [allegedly dishonest] disclosure statement").

As in *Small*, Medidata cannot prove that its employees saw the typed name that forms the sole basis of its forgery allegation because the emails were truncated and Medidata's employees did not recall expanding the emails. (SMF ¶ 26, Exh. 20, 27:03-10, 28:06-09; SMF ¶ 39, Exh. 21, 38:04-16; SMF ¶ 40, Exh. 19, 42:16-22). Because Medidata is unable to prove that its employees saw the alleged forgery (let alone that it impacted their decision-making), it cannot prove that the loss "resulted from" the alleged forgery and its claim fails as a matter of law.

III. <u>INSURING CLAUSE 6</u>: AN AUTHORIZED TRANSFER INITIATED AND EXECUTED BY AUTHORIZED SIGNATORIES IS NOT "FUNDS TRANSFER FRAUD."

Medidata seeks coverage under Insuring Clause 6 on the theory that its employees' decision to authorize a wire transfer constitutes **Funds Transfer Fraud**. Insuring Clause 6 expressly limits coverage to "direct loss of **Money** or **Securities** sustained by an **Organization** resulting from **Funds Transfer Fraud** committed by a **Third Party**." (SMF ¶ 10, Exh. 1, FIC001342). A wire transfer executed by employees authorized to effect such transfers cannot, as a matter of law, trigger such coverage because (1) a voluntarily approved transfer is not **Funds Transfer Fraud**, and (2) an employee is not a **Third Party** (as defined by the Policy).

A. A Knowing Transfer by Authorized Signatories Is Not "Funds Transfer Fraud."

Medidata's claim under Insuring Clause 6 ignores the plain definition of **Funds Transfer Fraud**. That term is defined as "fraudulent electronic, telegraphic, cable, teletype, facsimile, telephone or written instructions (other than **Forgery**), ***purportedly issued by an Organization***, and issued to a financial institution directing such institution to transfer, pay or deliver **Money** or **Securities** from any account maintained by such **Organization** at such institution, ***without such Organization's knowledge or consent***." (SMF ¶ 11, Exh. 1, FIC001345) (emphasis added). The phrases "purportedly issued by" and "without such **Organization's** knowledge or consent" distinguish involuntary transactions from fraudulently-caused voluntary transfers. Where, as here, an insured voluntarily executes a wire transfer (even if based upon a misrepresentation), Insuring Clause 6 does not apply. *Cumberland*, 958 N.Y.S.2d 306; *Pestmaster*, 2014 WL 3844627 at *6-7; *Northside Bank v. Am. Cas. Co.*, 60 Pa. D. & C. 4th 95 (Pa. County Ct. 2001).

The New York Supreme Court rejected Medidata's theory of coverage in *Cumberland*. An insured that invested money with Bernie Madoff sought coverage under its commercial crime policy on the theory that the loss resulted from an unauthorized transfer of money from its account. *Id.*, 958 N.Y.S.2d at 306. Summarily rejecting that claim, the court held that the funds transfer fraud insuring agreement did not provide coverage because Madoff was authorized to transfer the funds. *Id.* The fact that Madoff misused his authority and transferred money for personal gain was insufficient to trigger coverage.

Pestmaster also rejected Medidata's analysis. In that case, the insured voluntarily transferred funds to a third-party, but claimed that its loss was nonetheless covered under the funds transfer fraud insuring agreement on the theory that it was provoked to transfer the funds based upon fraudulent information conveyed through a computer. The district court rejected that claim, holding that a transfer by an authorized signor did not trigger coverage:

> Instead, it is undisputed that Priority 1 wrongly used the funds only after they had been transferred to Priority 1 pursuant to the express authorization granted to Priority 1 by Pestmaster. Therefore, Pestmaster has failed to demonstrate that it suffered a loss that was covered by the Funds Transfer Fraud Insuring Agreement.

2014 WL 3844627 at *6.

Funds Transfer Fraud coverage only applies in the event of a wire transfer sent or altered without the insured's knowledge. *Northside Bank* explained this distinction. In that case, a bank attempted to recoup the losses it had sustained after transferring funds to its customers based on credit and debit card authorizations that turned out to be false because the goods had never been delivered. The court held that the insured could not recover under Funds Transfer Fraud because "the purpose of the coverage was to protect the Bank from someone breaking into the electronic fund transfer system and pretending to be an authorized representative or altering the electronic instructions to divert monies from the rightful recipient." *Id.*, 60 Pa. D. & C. 4th at 101. That did not occur in *Northside Bank*, as the insured received valid electronic instructions. While based on fraud, the entry of the instruction by the insured precluded coverage. *Id.*

In this case, the wire transfer was not "purportedly" issued by Medidata; it was in fact issued by Medidata, through authorized signatories who voluntarily approved and executed a wire transfer. Medidata's representatives intentionally logged into Chase's banking system using unique logins/passwords, freely entered the wire transfer, and freely approved it. (SMF ¶ 32, Exh. 20, 13:20-14:16, 50:17-51:14, 53:06-54:20; SMF ¶ 48, Exh. 21, 32:10-25, 48:24-49:21; SMF ¶ 49, Exh. 19, 57:13-58:16). Their voluntary conduct constitutes an intentional act by Medidata. *Aetna Cas. & Sur. Co. v. Shuler*, 72 A.D.2d 591, 592 (App. Div. 1979) ("a corporation acts through its agents, whose acts are the acts of the corporation"); *Karaduman v. Newsday*, 416 N.E.2d 557, 568 (N.Y. 1980) (actions of "employees of the corporation acting within the scope of their employment would be deemed by the law to be the actions of the corporation").

The fact that Medidata would not have authorized the wire transfer had it known of the true purpose does not alter the fact that, at the time of the transfer, its employees were acting voluntarily and knowingly. *Advanced Aerofoil Technologies, AG v. Todaro*, 2013 WL 410873, at *8 (S.D.N.Y. Jan. 30, 2013) (use of system was authorized because employer never revoked privileges, despite the fact that the employees acted against the employer's interests). Because [redacted], [redacted] and [redacted] initiated and approved a knowing transfer, that transfer cannot constitute **Funds Transfer Fraud**, as defined by the Policy. (SMF ¶ 11, Exh. 1, FIC001345).

B. Insuring Clause 6 Does Not Apply to Transactions Effected by an Employee.

Medidata seeks to recover for a wire transfer exclusively initiated and approved by employees. (SMF ¶ 32, Exh. 20, 13:20-14:16, 50:17-51:14, 53:06-54:20; SMF ¶ 48, Exh. 21, 32:10-25, 48:24-49:21; SMF ¶ 49, Exh. 19, 57:13-58:16). Medidata admits that it directly employed every individual involved in the creation and execution of the wire transfer:

> 32. Employee 1 prepared the wire in the online system of Medidata's bank, and while Employee 2 and Employee 3 had questions for Employee 1, they both were ultimately convinced by the fraud that these funds were pursuant to a legitimate request by a Medidata executive, and approved the transfer.
> 33. Once Employees 2 and 3 approved the transfer, Medidata's bank executed the wire transfer based on the instructions provided by Employee 1 and the $4,770,226.00 was transferred.

(Dkt. 1, ¶¶ 32-33).

These admissions are fatal to Medidata's claim under Insuring Clause 6 because by its very terms, Insuring Clause 6 applies to "**Funds Transfer Fraud** . . . committed by a **Third Party**." (SMF ¶ 10, Exh. 1, FIC001342). The term **Third Party** is defined as "a natural person other than (a) an **Employee**; or (b) a natural person acting in collusion with an **Employee**." (SMF ¶ 5, Exh. 1, FIC001347). Medidata cannot, therefore, seek recovery for a transfer committed by an **Employee**;[15] it must prove that the transaction was effected by a stranger. *Id.*

[15] **Employee** includes a natural person in "the regular service of" Medidata, whom Medidata "compensates by **Salary**" and has the "right to govern and direct. . . ." (SMF ¶ 6; Exh. 1, FIC001344).

That did not occur here because the claimed transaction was, according to Medidata's complaint, effected by three "employees." (Dkt. 1, ¶¶ 32-33). While the complaint does not identify the individuals by name, Medidata admitted in discovery that the individuals who effected the wire transfer all regularly worked for Medidata, were paid by Medidata, and were directed by Medidata. (SMF ¶ 57, Exhibit 18, Medidata's Objections and Responses to Federal's First Requests for Admission, ¶¶ 1-3). These admissions, combined with undisputed deposition testimony, demonstrate that [redacted], [redacted] and [redacted] qualify as **Employees** (not as **Third Parties**) and thus, transactions effected by them do not trigger coverage under Insuring Clause 6.

CONCLUSION

For the reasons set forth herein, Federal Insurance Company respectfully requests that this Court grant summary judgment in its favor on the grounds that Medidata has not established a loss covered by Insuring Clause 4, 5, or 6 of the Policy, and for any other relief the Court deems necessary and appropriate.

Dated: August 13, 2015

Respectfully Submitted,

GORDON & REES, LLP

By: ______________________

Jeffrey Spiegel
Scott L. Schmookler
Sara Gronkiewicz-Doran
One North Franklin
Suite 800
Chicago, Illinois 60606
(312) 565-1400
Attorneys for Defendant
Federal Insurance Company

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on August 13, 2015, the foregoing Memorandum in Support of Motion for Summary Judgment (Redacted) was served on all counsel of record via the Court's ECF system.

Jeffrey Spiegel
Scott Schmookler
Sara Gronkiewicz-Doran
GORDON & REES LLP
1 North Franklin
Suite 800
Chicago, Illinois 60606
(312) 565-1400
jspiegel@gordonrees.com
sschmookler@gordonrees.com
sgronkiewicz-doran@gordonrees.com
Attorneys for Defendant
Federal Insurance Company